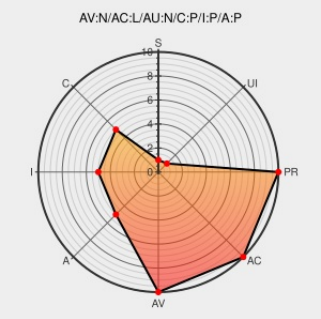
CVE-2005-1935

Published on: 06/09/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1935

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows 2000 from Microsoft contain the following vulnerability:

Heap-based buffer overflow in the BERDecBitString function in Microsoft ASN.1 library (MSASN1.DLL) allows remote attackers to execute arbitrary code via nested constructed bit strings, which leads to a realloc of a non-null pointer and causes the function to overwrite previously freed memory, as demonstrated using a SPNEGO token with a constructed bit string during HTTP authentication, and a different vulnerability than CVE-2003-0818. NOTE: the researcher has claimed that MS:MS04-007 fixes this issue.

CVE-2005-1935 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
kill-bill	Exploit web.archive.org text/xml Inactive Link Not Archived	MISC www.phreedom.org/solar/exploits/msasn1-bitstring/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF asn1-constructed-heap-overflow(20870)

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2000	All	sp2	All	All
Operating System	Microsoft	Windows 2000	All	sp3	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	fr
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows 2003 Server	64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	All	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Nt	4.0	sp6	terminal_server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	server	All
Operating System	Microsoft	Windows Nt	4.0	sp6a	workstation	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating	Microsoft	Windows Xp	All	sp1	tablet_pc	All

System						
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	gold	All	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	tablet_pc	All

cpe:2.3:o:microsoft:windows_2000:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp2:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp3:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2000:*:sp4:*:fr:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:64-bit:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_2003_server:r2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:workstation:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6:terminal_server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:server:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_nt:4.0:sp6a:workstation:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:*:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:gold:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:64-bit:*:*:*:*:*:

cpe:2.3:o:microsoft:windows_xp:*:sp1:tablet_pc:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→